


GREENVILLE POLICE DEPARTMENT POLICY AND PROCEDURES MANUAL		
<b>Chapter 82</b>	<b>Records</b>	
<b>Date Initially Effective 11/30/94</b>	<b>By The Order Of:</b>  <b>Hassan Aden, Chief of Police</b>	
<b>Date Revised 07/30/13</b>	<b>Date Reissued 07/30/13</b>	<b>Page 1 of 10</b>

### 82.1.1 RECORDS COMPONENT

CALEA Standard: 82.1.1, 82.1.2, 82.1.3, 82.1.4, 82.1.5

#### Privacy and Security

It is the policy of the Greenville Police Department to have a Records Section to meet the management, operational, and informational needs of the Department and to place accountability for the records function in a specific specialized component. The Records Section is a component of the Logistics Division and is responsible for the records function of the Greenville Police Department. The Records Section is in a secure area of the Police Department and is under the direct supervision of the Community Services Supervisor.

The purpose of this directive is to establish guidelines for the security of Greenville Police Department records and files consistent with public record laws and for the overall operation of the Records Section. Although most records are submitted electronically, the Records Section still maintains the capability of scanning original records of documents into the RMS storage system. Access to records shall be limited to authorized personnel in order to maintain security and to comply with North Carolina law. This procedure shall ensure the confidentiality, availability, access, and security of records maintained by the Greenville Police Department. The privacy and security of criminal history records shall be in accordance with the criteria set forth in U.S. Department of Justice regulations regarding access and review.

#### Records Accessibility

Records information is accessible to all operations personnel on a twenty-four (24) hour basis through the City of Greenville's electronic document storage system. Access to this system is governed by individual passwords that are changed every 90 days. Passwords must be six (6) characters in length and for security purposes must contain at least 3 of the following: one (1) uppercase character, one(1) lowercase character, one(1) special character or one (1) numerical value. Once records have been located by querying the computer system, authorized users have the option to print the selected report(s) at the document retrieval station.

#### Records Function

Under the supervision of the Community Services Supervisor, the functions of the Records Section include, but are not limited to:

- *Report Review:* The report review process will begin with platoon supervisors who will review and approve all field case reports after they have been electronically submitted. The Records Section will conduct another review of the electronically submitted reports. This final review will be for purposes of verifying that all documents submitted are accounted for and contain proper classification, disposition codes, and case numbers.
- *Report Access and Release:* The Records Section will control the availability and confidentiality of all reports and records to the public. Records access shall be limited to authorized personnel. Information released to the public shall be in accordance with North Carolina General Statutes regarding public information.

- *Records Maintenance:* The Greenville Police Department's RMS maintains electronically all police reports and records identified in this directive.
- *Records Retrieval:* The Records Section will use the case number reporting system for all filing and retrieval purposes. Information from state uniform citations is data entered and indexed by the defendant's name and citation number.

The Criminal Investigation Bureau Supervisors shall review submitted reports daily to determine those reports to be assigned for follow up investigation. All follow up investigative activities will be documented on supplemental investigative reports in a timely manner. All information and documentation relevant to the investigation shall be included and submitted as part of the record.

### **Juvenile Records**

North Carolina law requires that all law enforcement agencies take special precautions to ensure those law enforcement records concerning a juvenile are protected against disclosure to any unauthorized person.

The Greenville Police Department's juvenile arrest and criminal history records shall be maintained in the Records Section in a secure location. Juvenile arrest reports are completed electronically by officers in the field on the Juvenile Contact Form which is clearly printed at the top of the form. In the event a juvenile arrest report cannot be completed electronically it shall be recorded on the pink "Juvenile Contact Form" which is easily distinguished from other types of paperwork. Case investigations involving juveniles that are not completed electronically must contain the phrase "See Narrative" in the victim or suspect fields.

Juvenile photographs may be taken in certain circumstances with the appropriate Court Order using any digital imaging other than the mug imaging system. Photographs should be delivered to the Forensics Services unit for storage in a separate folder in the Digital Darkroom. Juvenile fingerprints may be obtained in certain circumstances with the appropriate Court Order. Juvenile fingerprint cards will be delivered to the Forensic Services Unit and notification made that they are associated with a juvenile case. Juvenile fingerprint cards will be stored in the Forensic Services Supervisor's office in a separate and secure filing cabinet.

Additional procedures relative to the collection, dissemination, retention, disposition and expungement of records and identification pertaining to juveniles are contained in Chapter 44, Section 44.2.2. *Taking a Juvenile Into Custody.*

### **Records Retention**

The Greenville Police Department follows the guidelines set forth in the *North Carolina Municipal Records Retention and Disposition Schedule* for all records.

### **Incident Base Reporting**

The Greenville Police Department participates in the North Carolina Uniform Crime Reporting System through incident based reporting. Statistical data is supplied to this program by records personnel. The Records Section shall prepare a report in electronic media format at the beginning of each month for mailing to the North Carolina Department of Justice. The report shall be submitted in a timely manner so that the report arrives at the Department of Justice not later than the fifteenth day of the month. Submission of the Uniform Crime Reports shall be the responsibility of the Community Services Supervisor or designee.

## **82.1.2 PROTECTING THE INTEGRITY OF COMPUTERIZED RECORDS**

CALEA Standard: 82.1.6, 11.4.4

### **Audit of Central Records Access**

The integrity and security of the central records files is dependent upon the access systems that provide control through a series of passwords and access codes. Employees are not permitted to use passwords, access a file, or retrieve any stored communication unless authorized to do so. The Information Technology Department of the City of Greenville maintains a current "Computer Security and Use Procedure". All employees of the Greenville Police Department are required to sign, acknowledge and comply with these procedures.

Specific requirements regarding computer access and passwords can be found in the Information Technology "Computer Security and Use Procedure" sections IV and V:

### **Computer System Access**

Computing resources, data, and information must be protected from unauthorized use, external intrusion, theft and accidental or malicious damage. To protect active sessions:

- A. Close down active sessions and use a password-protected screensaver to secure your terminal or workstation if you intend to leave it unattended or inactive. The example below is the correct way to immediately lock and unlock your workstation.  
(e.g., under Windows XP, press Ctrl-Alt-Del keys, then press Enter to lock the workstation. To unlock your workstation, move your mouse or press a key on the keyboard, press Ctrl-Alt-Del keys, then enter your password in the password field of the dialog box).
- B. Logoff the network and shut down or lock your computer at the end of the working day and on weekends unless otherwise instructed.
- C. Use secure network file locations to store all City data, unless there is a specific need or limitation requiring data to be stored on your computer's local hard drive (local drives are not backed up). Do not store sensitive information on your local hard drive unless it is protected by access controls. Contact the IT Department to discuss data encryption software options. Health information must be stored and protected on secure drives where backup, recovery, and retention are available and to meet HIPAA rules and regulations governing these electronic records.

### **Passwords**

Guard your password carefully. Adhere to the following guidelines:

1. Do not reveal passwords to anyone. If required to disclose current password to an authorized computer technician for system maintenance or troubleshooting, change your password immediately after maintenance is complete
2. Do not write down and post or store passwords near a workstation, under the keyboard or mouse pad, or other areas where they could be found and used.
3. For new accounts, change passwords upon first login or upon password reset for the account.
4. Change passwords immediately if it is suspected that they have been compromised.
5. Change passwords every 90 days. If greater security is required, change passwords more frequently. (Network passwords will expire automatically after 90 days.)
6. Change default passwords supplied with new software packages immediately after the software installation.
7. After five unsuccessful network login attempts (invalid user ID and/or password), the system will lock the user ID account. Contact the help desk if this occurs.

### **The following guidelines for choosing passwords should be used:**

1. Passwords must be composed of at least 6 characters. If the computer software in use does not support 6-character passwords, use the largest number of characters possible.
2. The password must not contain a user name or surname(s); avoid using easily guessed passwords such as those derived from initials, user ID, address, telephone number, license plate of your car, date of birth, spouse's name, children's names, pet's name, etc.
3. Passwords should be difficult to guess. A password must contain one letter in upper case (A,B,C,...Z), one letter in lower case (a,b,c,...z) and one digit (0,1,2,...9) as a minimum.

4. Do not reuse any of the previous 4 passwords.
5. If prompted to save passwords while using Internet Explorer, select "No".

The sign on procedures require the user to enter a name and password. The password is entered invisibly on the screen. Access to the menu selections are assigned to a particular user by the IT Department in conjunction with information provided by the Police Department Community Services Supervisor. The Information Technology Department monitors, on a regular, recurring basis, authorized passwords and access codes and observe for evidence of security violations.

The Logistics Division Lieutenant or designee shall notify the IT Department as necessary to remove a user from the mainframe system and to disable the User Profile. The Logistics Division Lieutenant or designee shall provide necessary information to the IT Department when a user will be replaced.

### **Outside Computer Software and Disk**

Section X and XI of the City of Greenville "Computer Security and Use Procedure" govern the introduction of computer software and data disks into agency-controlled computer systems and hardware:

#### **Software**

All employees shall comply with all legal obligations that relate to software copyright and licensing agreements. The City of Greenville provides a standard suite of supported software for use. If you require additional software, the following applies:

- IT support staff are responsible for the purchase, installation, and configuration of software/hardware for the City. Software intended for use on City of Greenville servers and other shared resources must be submitted for testing and verification to IT support staff **before installation**.
- Installation of any software must be approved by IT Support.
- Do not create or use an unlicensed copy of software.

#### **Virus Prevention and Detection**

- A. Any file received from an unknown source should be considered highly suspicious and deleted without opening.
- B. The following guidelines must be followed to minimize the impact of viruses:
  1. Ensure that installed virus protection software is not deliberately disabled or prevented from running.
  2. Scan all floppy disks, CD ROMs or other media originating from external sources. This includes media last used on a home computer, and media obtained from external business partners, training agencies, service technicians and vendors.
  3. Scan all software and electronic documents acquired from third parties and external networks.
  4. Scan all floppy disks before distributing to others.
  5. Report the suspicion of any virus to the IT support staff immediately.

#### **Files Backup and Storage**

Citywide computing systems backup and storage provisions are handled according to the "Information Technology Backup Strategy", COG Document # 788784.

### **82.2.1 FIELD REPORTING SYSTEM**

CALEA Standard: 82.2.1, 82.2.2, 82.2.3,

**Specific Reporting Requirements**

Records that document police activity shall include the following information:

- Date and time of the initial reporting
- Name (if available) of the citizen requesting the service, or the victim's or complainant's name
- Nature of the incident
- Nature, date and time of action taken (if any) by law enforcement personnel

Police officers investigating traffic collisions shall follow the procedures set forth in Chapter 61, TRAFFIC governing the use of report forms.

When conducting supplemental investigations the appropriate supplemental form must be used as identified in the *GPD FIELD REPORTING MANUAL*.

**Field Reporting Manual**

The Field Reporting Manual specifies the following information:

- The forms to be used in field reporting
- Procedures to be followed in completing field reports

Copies of the manual shall be disseminated to the following personnel and locations:

- Deputy Chief
- Criminal Investigations and Field Operations Bureau Commanders
- Platoon/Unit Lieutenants
- Field Training Officers
- Sergeant's Office
- Administrative Assistant's Office (Criminal Investigations Bureau)
- Accreditation

**Records Repository**

The Greenville Police Department's RMS maintains a repository of records filed sequentially by case numbers that includes:

- Offense reports
- Arrest reports
- Traffic collision reports
- Towed vehicle reports

**Reporting Requirements**

The following categories of incidents occurring within the jurisdiction of the Department shall be documented in reports, and/or entered into the Computer Aided Dispatch system:

- Citizen reports of crimes
- Citizen complaints
- Citizen requests for service when a police officer is dispatched; an employee is assigned to investigate; or an employee is assigned to take action later
- Criminal and non-criminal cases initiated by law enforcement officers
- Incidents involving arrests, citations, or summonses

A record shall be made of actions taken by law enforcement personnel in any of the above described circumstances, whether in response to a request for service or for self-initiated actions.

**Case Numbering System**

The Computer-Aided Dispatch (CAD) system generates a case numbering system with the following provisions:

- The CAD system is designed to automatically assign a sequential unique number (call number) to all incidents and a sequential unique case number to all incidents of law enforcement service requiring a case investigation, traffic investigation and/or arrest report.
- The CAD numbering system is designed to ensure that all cases receive a number and that numbers are neither omitted nor duplicated.

#### **Report Review Procedures**

Every report will be reviewed by a supervisor. The supervisor who reviews the report will place his/her signature on the report to indicate the supervisor has reviewed the report and has approved its contents for Departmental purposes. Supervisors shall check reports for accuracy, completeness, legibility, and neatness. Reports not approved will be returned to the police officer completing the report for required corrections. Supervisors reviewing electronically submitted reports will either select “approve” or “reject” before the report is submitted electronically to the Records Section as verification that they have reviewed the report. Electronically approved reports are automatically forwarded to the Records Section. Electronically rejected reports are shall be returned to the investigating officer for corrections before being electronically submitted to the Records Section.

### **82.2.2 DISTRIBUTION OF REPORTS AND RECORDS**

CALEA Standard: 82.1.1, 82.2.4

The Records Clerks shall process reports and records by merging the original documents into the Records Section RMS storage system. After the record is merged it is permanently stored in the RMS storage system.

#### **Internal Distribution**

The Special Investigations Supervisor and the Criminal Investigations Supervisors shall utilize the image retrieval stations to review reports and records for follow-up assignment. Supervisors will screen all cases and make case assignments in accordance with Greenville Police Department Policy and Procedures, Chapter 42, *Criminal Investigations*.

#### **External Distribution**

Copies of police reports will be provided to law enforcement/criminal justice agencies upon request. The information contained in the police report must be needed for performance of their law enforcement duties. The only exceptions to this rule are the Special Investigations case files.

The release of information from the Special Investigations case files must be authorized by either the investigating officer or the Special Investigations Supervisor.

The Greenville Police Department shall release the following records to the public upon request:

- Select pages of the incident reports
- Redacted arrest reports
- Redacted traffic collision reports
- Contents of Communications Center telephone recordings
- Contents of Communications Center radio tape recordings

Any audio recording that potentially releases victim information should be reviewed by the City Attorney’s Office prior to release.

All reports of incidents involving juveniles as either the victim or suspect, or incidents involving sex crimes shall have the names of the juvenile or the sex crime victim removed.

North Carolina GS 132-1.4 stipulates that records of criminal investigations or records of criminal intelligence information are not public records with the following exceptions:

- The time, date, location, and nature of a violation or apparent violation of the law reported to a public law enforcement agency
- The name, sex, age, address, employment, and alleged violation of law of a person arrested, charged, or indicted
- The circumstances surrounding an arrest, including the time and place of the arrest, whether the arrest involved resistance, possession or use of weapons, or pursuit, and a description of any items seized in connection with the arrest
- The contents of 911 and other emergency telephone calls received by or on behalf of public law enforcement agencies, except such contents that reveal the name, address, telephone number, or other information that may identify the caller, victim, or witness
- The contents of communications between and among employees of public law enforcement agencies that are broadcast over the public airways
- The name, sex, age, and address of a complaining witness

Greenville Police Department personnel may temporarily withhold the name or address of a complaining witness pursuant to North Carolina General Statute 132-1.4, if release of the information is reasonably likely to pose a threat to the mental or physical health or personal safety of the complaining witness or materially compromise a continuing or future criminal investigation or criminal intelligence operation. Information temporarily withheld pursuant to GS 132-1.4 shall be made available for release to the public upon request as soon as the circumstances that justify withholding it cease to exist.

The Greenville Police Department may release other records not categorized as confidential to the public upon request.

### **82.3.1 RECORDS INDEX**

CALEA Standard: 82.3.1, 82.3.2

#### **Master Name Index (Global Jacket)**

An alphabetical master name index is maintained through the computer system. The master name index includes names of persons identified in incident reports, supplemental reports, arrest reports, traffic collision reports and traffic citations. The following types of people meet the criteria for inclusion into the master name index:

- Victim
- Complainant
- Suspect
- Arrestee
- Witness
- Injured (traffic collision related)
- Other
- Persons of Interest

#### **Calls for Service Records**

The Greenville Police Department maintains a computerized database containing records that include service calls, crimes by type, and crimes by location. This information is available to all Department personnel via computerized query.

#### **Stolen, Found, Recovered, and Evidentiary Property Index**

The Property & Evidence Unit maintains a record of all found/recovered property, evidentiary property, property retained for safekeeping, and property to be destroyed. All property received by the Property & Evidence Unit is recorded in the computerized "Crimes Management System's Evidence/Property Tracking" section by the Property

& Evidence Unit. The Property Report is filed in the Property & Evidence Unit as outlined in Chapter 84 of the Greenville Police Department Policy and Procedures Manual

Prior to submitting the property or evidence to the Property & Evidence Unit, police officers shall request a query of the DCI/NCIC files for any property that has a unique identifying number to determine if the property has been reported stolen. Stolen property will be cleared/located from the DCI/NCIC files in accordance with DCI Regulations.

### **82.3.2 TRAFFIC RECORDS SYSTEM**

CALEA Standard: 82.3.3, 82.3.4

The Greenville Police Department utilizes various systems to maintain or have access to traffic information to include:

- Traffic collision data, (reports, investigations, and locations)
- Traffic enforcement data, (citations, arrests, dispositions, and locations)
- Report of roadway hazards and hazardous conditions

The traffic records system provides accurate information including locations of traffic collisions and citations to field personnel and provides data upon which management decisions can be based.

Greenville Police Department Policy and Procedures Manual, Chapter 61, *Traffic*, identifies data to be collected, analyzed, and disseminated relative to traffic records.

#### **Citation Forms**

##### **Issuing Citation Books**

The Field Operations Bureau Administrative Assistant shall obtain uniform state citation books from the Clerk of Court as needed. Uniform state citation books shall be stored in a secured area with restricted access. Platoon commanders or supervisors shall contact the Field Operations Bureau Administrative Assistant to obtain state uniform citation books which are then assigned to the requesting supervisor. The Field Operations Bureau Administrative Assistant shall record the control numbers from each uniform state citation book issued and the date issued. The requesting supervisors shall issue citation books to the police officers and shall maintain a log of citation books assigned to police officers.

##### **Accounting for Citations and Citation Books**

Police officers are accountable for the citation books issued to them. Citations are cross-referenced by the issuing police officer's name and date of issuance.

The original and "Driver License Section" copies are returned to the Clerk of Courts Office. The offender receives the pink copy. The police officer retains the "Officer's Copy". One copy is left in the citation book for control purposes. If a police officer makes an error while writing a citation, or if a citation has become damaged due to accidental exposure to rain, snow, etc, the police officer may write "Void" across the original citation and on all copies. The original and all copies of the citation are to be left in the citation book.

If a citation or citation book is lost or stolen, the police officer shall immediately notify the police officer's on-duty supervisor. The police officer shall write and submit a memorandum that explains the circumstances of the loss. The citation control number(s) should be identified in the memorandum. If either a citation or a citation book is missing, a copy of the memorandum submitted by the police officer should be taken to the Clerk of Court's office.

The police officer shall return used citation books to the on-duty supervisor. The supervisor shall inspect the used citation book to ensure that all necessary copies are accounted for, and record the used citation book as being returned next to the name of the police officer submitting the book. The supervisor shall verify that all of the



yellow copies of the citations have been left in the citation book prior to returning the used citation books to the Field Operations Bureau Administrative Assistant.

Additional policy and procedures relative to the preparation and accountability for Uniform Traffic Citations is presented in Greenville Police Department Policy and Procedures Manual, Chapter 61, Section 61.1.2 *Traffic*.

### **82.3.3 OPERATIONAL COMPONENT RECORDS**

CALEA Standard: 82.3.5

Operational records are maintained as follows:

- The Greenville Police Department's RMS shall be the central repository for all offense and incident reports, arrest reports, other field reports, and other official records.
- The Special Investigations Unit shall maintain a secured file containing Greenville Police Department Intelligence and Informant activities.
- The Juvenile Section shall maintain only working files of current investigations concerning juveniles.
- The Administrative Services Bureau shall maintain the Department's personnel records and training records.

### **82.3.4 CRIMINAL IDENTIFICATION AND HISTORY**

CALEA Standard: 82.3.6, 82.1.7

#### **Criminal History File**

The Department database includes a criminal history file maintained on every person arrested by the Department. The file can include:

- Fingerprint card
- Criminal history transcripts (state and federal)
- Photograph (if available)
- Copy of arrest reports

Arrestee criminal history file information is maintained in at least one of the following locations:

- North Carolina State Bureau of Investigation, Division of Criminal Information (DCI)
- Police Department case file
- Clerk of Court's office
- Greenville Police Department Identification Section

All information subject to inclusion in an arrestee's criminal history file is accessible through the DCI terminal and is cross-referenced according to a number of descriptors including, but not limited to:

- Name
- Case number
- FBI number
- SID number

#### **Arrest Identification Number**

The Greenville Police Department's RMS automatically assigns a global jacket (I.D.) number to each person custodially arrested. All subsequent arrests and other information concerning that person should be referenced to his or her identification number. Each person will have only one identification number. The Community Service Supervisor shall ensure that numbers are not skipped or duplicated. The following procedures will apply:

Upon receipt of an arrest form, the records section data entry clerk will perform a computer inquiry by name and/or social security number for the arrestee to determine if a Department I.D. number has previously been

assigned to the arrestee. If a Department I.D. number has been previously assigned to the arrestee, the data entry clerk will enter the number on the arrest form in the appropriate field. If a Department I.D. number has not been previously assigned to the arrestee, the data entry clerk will assign a number using the consecutive numbering machine provided for that purpose. The data entry clerk will then enter the arrest data, along with the assigned I.D. number, into the appropriate computer files.

**Access and Dissemination of Criminal History Records**

The State Bureau of Investigation (SBI) Division of Criminal Investigative Records (DCI) maintains a computerized criminal history of individuals who have been arrested and/or for which the SBI has a valid criminal fingerprint card.

Access is restricted to DCI authorized law enforcement/criminal justice agencies and personnel. Personnel accessing DCI records must complete DCI certification requirements, obtain a DCI Operator Identifier and password, and must be under the management control of an agency assigned an Access Identifier (ORI). DCI certification is valid for two years. Re-certification is necessary for continued DCI access and/or terminal operations.

DCI provides an automated log of criminal/investigative inquiries. The automated log will contain the information supplied by the operator in the inquiry screen. Secondary dissemination to any person outside the initial requesting agency must be indicated in the inquiry screen or in the case file pertaining to that record. All inquiries and disseminations must comply with all DCI rules regarding access and dissemination. Any misuse or possible violations must be reported to DCI. Violations may result in loss of access and/or fines to the agency.

The NC SBI DCI module, *INTRODUCTION TO DCI NETWORK; STUDENT OUTLINE AND EXERCISE WORKBOOK*, identifies all regulations and requirements for DCI certification, access, and dissemination of criminal histories.